Amendment To The Specification

Please amend the specification as follows:

[0039] Continuing to refer to FIG. 3A, integrity check of a document received by a recipient at a destination device, such as facsimile apparatus 361, is made by decrypting the encrypted checksum and comparing this decrypted checksum with a checksum of the document received by facsimile apparatus 361. In the event of a mismatch, a portion of the document received by facsimile apparatus is clearly marked to denote that the received document has been tampered with. For example, in step 362, a digital storage is processed. In step 363, the integrity check is performed and in step 364, the fax is printed and may be flagged.

[0040] FIG. 3B illustrates a process overflow for security verification of a document received by a computer system which includes a facsimile communication system and related software. Digital data transmitted by an originating device, such as facsimile apparatus 210 or computer system 260, is received and stored in digital storage 392 of the computer system 391. Integrity check of a document received by a recipient at a destination device, such as computer system 391, is made by decrypting the encrypted checksum and comparing the decrypted checksum with a checksum of the data received by the computer system 391. In the event of a mismatch, data received by the computer system 391 and configured to be displayed using facsimile viewing software is clearly marked to denote that the received data has been tampered with. For example, in step 392, a digital storage is processed. In step 393, the integrity check is performed and in step 394, the fax is displayed with such status indication.